MANUAL DE CARGOS

Dependencia:	División Control Operativo	**Área**	Área Seguridad Operativa Informática
Código del Cargo:	3035.	**Código del Puesto:**	3035
Categoría	23	**Nombre del Puesto:**	Jefe de Área 2 TI
Nombre del Cargo:	Jefatura Seguridad Operativa Informática	**Reporta a:**	Jefe División Control Operativo
Objetivo del Cargo:	Planear, coordinar y administrar los servicios de Seguridad Operativa Informática en la organización, con el fin de garantizar una seguridad razonable en todas las operaciones realizadas, participando en el establecimiento de controles que permitan dar garantía en el cumplimiento de los procesos, normas, reglas, políticas y estándares definidos que aseguren una adecuada protección de los recursos informáticos.		

MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES
			1. Validar los procedimientos específicos de los contratos formales con los proveedores, así como monitorear la prestación de sus servicios.
			2. Monitorear periódicamente la efectividad de los controles internos a través de auto evaluaciones y/o auditorías, velar que éstos se cumplan de acuerdo con los requerimientos de seguridad establecidos.
			3. Dirigir, supervisar y orientar al personal a cargo, así como desarrollar actividades de planificación, organización, ejecución, control e integración de las tareas propias del área.
			4. Preparar informes de la gestión del área a cargo, documentación y respuestas a informes de Auditoría Interna, Externa, SUGEF y otros organismos a los que la Institución sea sujeta de fiscalización.
			5. Definir y cumplir en concordancia con los objetivos estratégicos, los objetivos y metas planteadas por el área, así como resolver nuevos retos que se presenten.
			6. Evaluar el desempeño de los servicios prestados por proveedores externos, así como verificar los informes de capacidad y desempeño.
			7. Coordinar los procesos de atención de reportes de solicitudes de usuarios de las plataformas tecnológicas referentes a asuntos de seguridad de la información.
			8. Velar por la existencia de un control de los activos del área.
			9. Planear, ejecutar, coordinar y controlar el presupuesto del área.
			10. Cumplir y hacer cumplir con lo que establecen las leyes vigentes (Ley de Control Interno).
			11. Acatar y velar por el cumplimiento constante de políticas, normativas, reglamentos y procedimientos relacionados.
			12. Ejecutar otras tareas propias del puesto.
			FUNCIONES ESPECÍFICAS
			13. Desarrollar planes de seguridad informática, así como coordinar, revisar, definir, implementar y administrar los esquemas de seguridad para las plataformas tecnológicas de la Institución.
			14. Establecer controles técnicos que permitan desde el punto de vista de seguridad de la información, una seguridad razonable en cuanto a la integridad y disponibilidad de las plataformas tecnológicas del Banco.
			15. Coordinar labores para establecer controles de protección a equipos físicos o virtualizados de la plataforma tecnológica del Banco.
			16. Coordinar labores para dar protección adicional a aplicaciones claves en la Institución, tales como procesos de análisis de vulnerabilidades, procesos de hardening y seguimiento de sus atenciones.
			17. Coordinar la definición y actualización de controles de seguridad de la información para el resguardo de activos sensitivos y de la tecnología de seguridad informática.
			18. Organizar y establecer labores de monitoreo y análisis de tendencias del ciberespacio, del panorama global de amenazas informáticas y su evolución, con el fin de analizar su impacto en la organización, así como sus remediaciones o medidas requeridas.
			19. Definir, desarrollar y velar por el cumplimiento del Reglamento, Manual y Políticas de Seguridad Informática, de acuerdo a mejores prácticas internacionalmente aceptadas en esta materia.
			20. Revisar, gestionar y mantener actualizadas las políticas, normativas, procedimientos, reglamentos relacionados con la seguridad informática y aspectos de control interno para proteger los recursos informáticos.
			21. Coordinar a nivel interdepartamental los proyectos tecnológicos, así como monitorear el buen uso de los recursos del área, por parte de los funcionarios desde el punto de vista de seguridad de la información.
			22. Realizar procesos de análisis y mitigación de los riesgos que se generan en el ámbito tecnológico desde el punto de vista de seguridad informática.
			23. Establecer el diseño en las arquitecturas de seguridad para las infraestructuras tecnológicas del Banco, consideradas como parte del desarrollo de proyectos e iniciativas del Conglomerado.
			24. Definir controles de seguridad informática, para ser establecidos a nivel de la infraestructura tecnológica del Banco y la definición de los planes de pruebas para las tecnologías del Banco o emergentes.
			25. Apoyar en los procesos de concientización sobre la importancia de la seguridad operativa de la información.
			26. Establecer y coordinar el monitoreo proactivo a nivel de seguridad operativa de la infraestructura tecnológica del Banco y sus competencias.
			27. Apoyar en la definición y ejecución de labores para todo caso relacionado con accesos e incidentes de seguridad de la información.
			28. Asesorar a otras áreas todo lo concerniente a seguridad operativa informática, para la adquisición de nuevas herramientas de software y hardware.

			FUNCIONES RELACIONADAS CON RIESGO
			29.Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			30.Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			31.Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			32.Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			33.Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			34.Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			35.Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			36.En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
			FUNCIONES RELACIONADAS CON SUGEF
			Según el Acuerdo SUGEF 14-17 “Reglamento General de Gestión de la Tecnología de Información”, el cual establece los requerimientos mínimos para la gestión de tecnología de información que deben de acatar las entidades supervisadas y reguladas del sistema financiero costarricense y en concordancia con la Ley de Control Interno, Capítulo III, Sección I “Deberes del jerarca y los titulares subordinados”, capítulo 12,13 y 14, este puesto es responsable del desarrollo de las actividades y tareas que le asignen velando por un adecuado ejercicio del mismo, debe garantizar la eficiencia y eficacia de las operaciones que le corresponde ejecutar tomando las medidas correctivas en beneficio de la institución. Por el nivel del puesto deberá promover mecanismos y procesos que mejoren el sistema de control interno en la gestión que le corresponde realizar. Así mismo, le corresponde evaluar el funcionamiento del área a cargo, tomar medidas para garantizar el cumplimiento de la gestión, asignar funciones y responsabilidades de los funcionarios a cargo y proporcionar los canales adecuados de comunicación para que los procesos se lleven a cabo de conformidad con el ordenamiento jurídico y técnico aplicable. Debe procurar mantener las operaciones con un nivel de riesgo aceptable.
CODIGO	**REQUISITOS EXIGIBLES**		
	Formación Académica:	Licenciatura en Ingeniería de Sistemas u otra carrera afín relacionada con las funciones del puesto. Preferiblemente con Maestría en un área afín con las funciones específicas del puesto	
	Legales:	Incorporación al Colegio de Profesionales respectivo.	
	Experiencia:	Tres años de experiencia en actividades propias a las descritas.	
CODIGO	*** REQUISITOS TÉCNICOS EXIGIBLES**		
	Contar al menos con una especialización certificada y vigente en materia de seguridad de la información, tales como:		
	1. Certified Ethical Hacker (CEH)		
	2. Certified Information Security Manager (CISM)		
	3. Certified Information Systems Security Professional (CISSP)		
	4. Certified CompTIA Security+		
	5. CSX Practitioner		
*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.**			
CODIGO	**REQUISITOS TÉCNICOS DESEABLES**		
	1. Conocimiento en Inglés Técnico (comprensión y lectura).		
	2. Conocimiento de las leyes aplicables al Conglomerado de normativa interna, reglamentos, directrices y circulares que regulan la actividad del Conglomerado.		
	3. Conocimiento en Contratación Administrativa.		
	4. Conocimiento en Gestión de seguridad de la información y su normativa interna.		
	5. Conocimiento en Gestión de seguridad de la información y riesgos.		
	6. Conocimiento en Ingeniería y administración de la Seguridad de la información.		
	7. Conocimiento en Seguridad en Telecomunicaciones (diseño y protección de la seguridad de redes).		
	8. Conocimiento en Seguridad en Sistemas Operativos (versiones recientes Microsoft Windows y Solarios) y Base de Datos (SQL y ORACLE).		
	9. Conocimiento en Control de Acceso y Gestión de la Identidad.		
	10. Conocimiento en Diseño, ejecución y análisis de pruebas de seguridad.		
	11. Conocimiento en Operaciones de Seguridad, Gestión de Incidentes y análisis forense.		
	12. Conocimiento en Servicios de Monitorización de los Procesos y Eventos de Seguridad de la Información.		
	13. Conocimiento en Seguridad en el Desarrollo de Software (ciclo de vida de desarrollo de software).		
	14. Conocimiento en Aplicaciones Web (OWASP).		
	15. Conocimiento en los estándares ISO 27000.		
	16. Conocimiento en el estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS).		
	17. Conocimiento en la Ley de delitos informáticos y norma SUGEF 14-09.		
	18. Redacción de Informes Ejecutivos y Técnicos.		
CODIGO	**SISTEMAS UTILIZADOS**		

	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL: JEFATURAS SOPORTE			
CÓDIGO	**Cardinales:**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CÓDIGO	**Gerenciales:**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CÓDIGO	**Del Negocio:**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CÓDIGO	**Del Soporte:**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CÓDIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Este perfil se aprueba con oficio GGC-1028-2018 de la Gerencia General Corporativa (Acta DGCA-Act.08-2018 (División Gestión de Calidad). Se incluyen Funciones de Riesgo las cuales se incorporan a los perfiles con la aprobación de la Gerencia General Corporativa, emitida en el HT-493-GGC-2019, de fecha el 14 de octubre 2019. Referencia: DIRGE-689-2019 / DIRCH-1477-2019.**				